EXHIBIT B

[redacted]

[redacted]

MEMORANDUM FOR: Director, Office of Security

VIA: Chief, Special Activities Staff
Personnel Security Group
Office of Security

FROM: Deputy Assistant Director of CIA for
Counterintelligence

SUBJECT: [redacted] Request for Administrative Leave
for [redacted] Michael [redacted]
AIN: [redacted]

1. [redacted] **Action Requested:** CIMC requests enforced administrative leave for Michael [redacted], a current CCI/COG employee who is associated with the investigation into the theft and unauthorized disclosure of Center for Cyber Intelligence (CCI) classified information published by Wikileaks beginning in March 2017, also known as "Vault 7."

2. [redacted] **Justification:** Michael [redacted]'s lack of cooperation with inquiries into his past activities with the primary person of interest in the FBI investigation and his unexplained activities on the computer system from which the CCI data was stolen, known as the "DevLAN," and raises significant concern about his truthfulness, trustworthiness, and willingness to cooperate with both routine OS reinvestigation processes and the criminal investigation into the left from his office. CIMC believes curtailing his access to CIA spaces and data systems is necessary to safeguard against potential future losses of sensitive and classified information.

[redacted]

DEFENDANT'S
EXHIBIT
L
S2 17 Cr. 548 (PAC)

[redacted]

SUBJECT: [redacted] Request for Administrative Leave for
Michael [redacted], AIN: [redacted]

3. [redacted] **Background**: Michael entered on duty in [redacted] 2011 as a student trainee in the Engineering Development Group (EDG) in what is now the Center for Cyber Intelligence. He converted to staff status in 2013, and remained in EDG until moving to CCI/COG in the summer of 2016. Michael is a software exploit developer with highly sensitive accesses. Michael was of interest in early 2016 to OS/Special Investigations Branch (SIB) in connection with an investigation involving two other CCI/EDG employees, Joshua Schulte and Amol [redacted], who reportedly had a physical altercation within EDG spaces. Schulte alleged that Amol had threatened his life, and Michael was interviewed as an informant. Michael reportedly also had had a physical altercation with Schulte in the workplace, and SIB interviewed him and an attempt to gain details. Michael, however, was not cooperative and refused to discuss his prior altercation with Schulte. Ultimately the SIB investigation did not substantiate the threat of physical harm to Schulte and the case was closed when Schulte resigned from CIA in November 2016. At the time, Schulte perceived himself to be victimized by Amol and was angered that CIA management did not do more to protect him. No action was taken against Michael with respect to his lack of cooperation with SIB.

4. [redacted] In February 2016, OS initiated [redacted] reinvestigation processing, which remains open at this time. Michael underwent two sessions of polygraph testing in May 2017 but did not clear all issues. In the wake of the theft and unauthorized disclosure of CCI's cyber toolkit on Wikileaks, CIMC requested that OS pause all ongoing security processing involving individuals who had access to the stolen data pending further investigation of the incident by CIMC and FBI. Michael's processing was paused as a part of that effort, as he held systems administrator privileges on the DevLAN, the system from which the toolkit was stolen, and was present in EDG spaces during the timeframe of the theft.

Investigation

5. [redacted] In support of the ongoing criminal investigation, CIMC conducted comprehensive reviews of all individuals who could have perpetrated the theft of the CCI

data, including Michael [redacted]. Several concerns about Michael have emerged in this review, including his close proximity to the theft of the data and his relationship with Joshua Schulte, the individual charged with the theft of data. Forensic analysis of Michael's activity on the DevLAN suggests that Michael may have additional knowledge of anomalies on the system at the time of the theft. Additionally, recent inquiries indicate Michael is still withholding relevant information concerning the circumstances surrounding the theft.

Risk Assessment

6. [redacted] Given the magnitude of the theft of the CCI toolkit and it's concomitant damage to national security, CIMC views Michael's lack of cooperation as a significant and untenable risk to the security of the operations on which he now works and any new tools he deploys for CCI. Michael, whatever his reasoning, has not complied with routine inquiries by SIB and during polygraph, and has failed to provide clear and verifiable information concerning his activities in the workplace around the time of the theft. Michael's behavior suggests that he has knowledge of details of the theft that he has not divulged. Michael's behavior suggests a lack of concern for the loss and a lack of commitment to comply with the basic security agreements he entered into upon hire. For these reasons, CIMC assesses that Michael's continued presence in the workplace is incompatible with best practices for security and insider threat mitigation.

Next Steps

7. [redacted] CIMC requests that the Office of Security:

- Immediately deactivate or block Michael's badge so that he may not gain access to CIA facilities;
- Place Michael on enforced administrative leave until the investigation into his knowledge of the theft of the CCI cyber toolkit is resolved.

SUBJECT: [redacted] Request for Administrative Leave for
Michael [redacted], AIN: [redacted]

CONCUR:

____________________________________ ______________________
Chief, Special Activities Staff Date

APPROVED:

____________________________________ ______________________
Director, Office of Security Date

[redacted]

SUBJECT: [redacted] Request for Administrative Leave for
Michael [redacted], AIN: [redacted]

[redacted]

Distribution:
Orig. - Addressee
1 - C/SC
1 - C/SAS
1 - C/CIC Chron
1 - Subject file
1 - CIC/[redacted] Chron

[redacted]